



Y. KOMATSU  
Filed 8-7-03  
1051

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 2 年    8 月    8 日  
Date of Application:

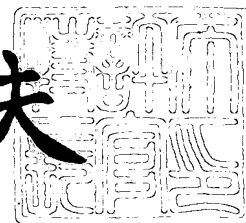
出 願 番 号            特 願 2 0 0 2 - 2 3 1 8 0 6  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 2 - 2 3 1 8 0 6 ]

出      願      人            N E C ビ ュ ー テ ク ノ ロ ジ ー 株 式 会 社  
Applicant(s):

2 0 0 3 年    7 月 2 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 0 5 9 5 3 8

【書類名】 特許願

【整理番号】 21110140

【提出日】 平成14年 8月 8日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/30

G06F 15/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 3 7 番 8 号

エヌイーシービューテクノロジー

ー株式会社内

【氏名】 小松 義治

【特許出願人】

【識別番号】 300016765

【住所又は居所】 東京都港区芝五丁目 3 7 番 8 号

【氏名又は名称】 エヌイーシービューテクノロジー株式会社

【代理人】

【識別番号】 100084250

【弁理士】

【氏名又は名称】 丸山 隆夫

【電話番号】 03-3590-8902

【手数料の表示】

【予納台帳番号】 007250

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0008450

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子機器及びその不正使用防止方法並びにその不正使用防止プログラム

【特許請求の範囲】

【請求項 1】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するためのインタフェースと、

該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記インタフェースを介して接続されている外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 2】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するためのインタフェースと、

該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記インタフェースを介して接続されている外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能

制限のうち前記装置特定情報と関連する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 3】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする手段と、

該暗証キーを記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 4】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、前記記憶手段に記憶されている暗証キーの装置特定情報及び接続経路情報と一致するか否かを判断する判断手段と、



前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 5】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけた情報を暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する手段と、

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限のうち前記装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 6】 自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、

外部装置を接続するための少なくとも二つのインタフェースと、

該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、

該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、

該暗証キーを少なくとも一つ記憶する記憶手段と、

前記各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーと一致するか否かを判断する判断手段と

前記判断手段が一致すると判断した場合に、前記機能制限手段が設定する機能制限のうち前記装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器。

【請求項 7】 前記外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる手段をさらに有することを特徴とする請求項 1 から 6 のいずれか 1 項記載の電子機器。

【請求項 8】 前記判断手段が判断を行ってから所定の時間が経過した後に、前記機能制限を再設定する手段をさらに有することを特徴とする請求項 1 から 7 のいずれか 1 項記載の電子機器。

【請求項 9】 外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 1 の装置特定情報取得工程と、

前記機能制限と前記第 1 の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 2 の装置特定情報取得工程と、

前記第 2 の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否か判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項 10】 外部装置を接続するためのインタフェースを備えた電子機

器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限のうち、前記第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項11】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する記憶工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から装

置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報の組み合わせが、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項12】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記外部装置が、前記第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを組にした情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、

前記外部装置が、前記第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報と、前記第2の接続経路情報との対が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において



設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項 13】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用防止方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 1 の装置特定情報取得工程と、

前記各機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 2 の装置特定情報取得工程と、

前記第 2 の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、

判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限のうち、前記第 2 の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行することを特徴とする電子機器の不正使用防止方法。

【請求項 14】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正利用防止方法であって、

電子機器が、

自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第 1 の装置特定情報取得工程と、

前記外部装置が、前記第 1 の装置特定情報取得工程においていずれのインタフ

エースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する第1の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、

前記外部装置が、前記第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報及びこれに関する第2の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限のうち前記第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法。

【請求項15】 前記第1の装置特定情報取得工程の後段に、前記第1の装置特定情報取得工程において前記電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程をさらに有することを特徴とする請求項9から14のいずれか1項記載の電子機器の不正使用防止方法。

【請求項16】 前記判断工程の実行後所定の時間が経過した時点で、前記機能制限を再設定する工程をさらに有することを特徴とする請求項9から15のいずれか1項記載の電子機器の不正使用防止方法。

【請求項17】 外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能

制限を設定する機能制限工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記機能制限と前記第1の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項18】 外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器の機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、

該各暗証キーを記憶手段に記憶する工程と、

前記インタフェースを介して前記電子機器に接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において

設定した機能制限のうち、前記第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項19】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、  
電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する記憶工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報の組み合わせが、前記記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項20】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、  
電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記外部装置が、前記第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経

路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶する工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、

前記外部装置が、前記第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報と、前記第2の接続経路情報との対が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項21】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、

電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、

該暗証キーを記憶手段に記憶させる工程と、

前記インタフェースのいずれかを介して前記電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報が、前記記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、

判断工程において一致すると判断した場合に、前記機能制限工程において設定

した機能制限のうち、前記第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラム。

【請求項22】 外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、  
電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、

前記外部装置が、前記第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、

前記機能制限と、所定の装置特定情報及びこれに関する第1の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、

該暗証キーを少なくとも一つ記憶手段に記憶させる工程と、

前記インタフェースのいずれかを介して前記電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、

前記外部装置が、前記第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、

前記第2の装置特定情報取得工程において取得した装置特定情報及びこれに関する第2の接続経路情報との対が、前記記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、

前記判断工程において一致すると判断した場合に、前記機能制限のうち前記第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特

徴とする電子機器の不正使用防止プログラム。

【請求項 2 3】 前記電子機器を制御する実質的なコンピュータに、前記第 1 の装置特定情報取得工程において前記電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程を、前記第 1 の装置特定情報取得工程の後段においてさらに実行させることを特徴とする請求項 1 6 から 2 2 のいずれか 1 項記載の電子機器の不正使用防止プログラム。

【請求項 2 4】 前記電子機器を制御する実質的なコンピュータに、前記判断工程の実行後所定の時間が経過した時点で、前記機能制限を再設定する工程をさらに実行させることを特徴とする請求項 1 6 から 2 3 のいずれか 1 項記載の電子機器の不正使用防止プログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、使用権限のない者の不正な使用を防止した電子機器及び電子機器の不正な利用を防止する方法及びそのプログラムに関し、特に、接続された外部装置を物理的な鍵として不正な使用を防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムに関する。

【0 0 0 2】

【従来の技術】

従来、電子機器を不特定多数人が使用可能な環境に設置する場合には、盗難や情報の盗用を防止するための対策を施す必要があった。

【0 0 0 3】

例えば、電子機器自体の盗難を防止するために、電子機器をワイヤやチェーン等で机などに固定し、電子機器を設置位置から所定範囲内でしか移動できないようにすることがある。

【0 0 0 4】

また、情報の盗用を防止するために、電子機器にパスワードを設定して、パスワードを知らない者が電子機器を利用できないようにすることがある。同様の目

的で、ユーザ認証用の装置（例えば、カードリーダー）を接続又は内蔵したりして、情報の盗用を防止することもある。

#### 【0 0 0 5】

しかし、電子機器をワイヤなどを用いて固定していても、ワイヤやチェーンを切断すれば電子機器を盗むことはできてしまう。また、電子装置の筐体にワイヤやチェーンなどを取り付けるための構造を設けなければならないため、装置の外観をデザインする上で制約を受けることとなる。

#### 【0 0 0 6】

また、電子機器にパスワードを設定した場合でも、例えば“over shoulder crack”（パスワードの盗み見）などによってパスワードが漏洩してしまうと、本来情報に対してアクセスする権限がない利用者が情報に不正にアクセスし盗用することができてしまう。

#### 【0 0 0 7】

さらに、情報の盗用を試みようとする者は、時間さえ十分にあればブルートフォースアタック（総当たり攻撃）によってパスワードを解読してしまうことも可能である。

パスワードを設定する者が十分な知識を備えていれば、他人に解読されにくいパスワードを設定することも可能ではある。しかし、他人に解読されにくいパスワードとはすなわち桁数が多く複雑なパスワードであるため、電子機器に関する知識に乏しい者にとっては利用しやすいものではない。例えば、パスワードの設定者自身がパスワードを忘れてしまい、電子機器を利用できなくなる可能性がある。

#### 【0 0 0 8】

加えて、電子機器にカードリーダーなどのユーザ認証用の装置を接続又は内蔵することは、電子機器自体やこれを適用したシステムの価格の上昇を招くことになる。加えて、PDAを適用した小規模なシステムにおいては、システムにユーザ認証用の装置を組み込むことが難しいこともある。

#### 【0 0 0 9】

このように、従来は、電子機器の盗難や情報の盗用を防止するために十分な対



策が取られているとはいえなかった。

#### 【0010】

コンピュータシステムにおけるセキュリティーの向上を目的とした従来技術として、特開平10-49493号公報に開示される「コンピュータシステム」がある。

このコンピュータシステムでは、コンピュータ本体及び周辺装置に識別番号を登録するための不揮発メモリがそれぞれ搭載されている。コンピュータ本体に周辺機器が接続されると、コンピュータ本体は、接続された周辺機器から登録番号を取得し、コンピュータ本体の登録番号と一致するか否かを判断し、コンピュータ本体の登録番号と一致する周辺機器のみを使用可能とするものである。

#### 【0011】

##### 【発明が解決しようとする課題】

しかしながら、上記公報のコンピュータシステムは、コンピュータ本体に接続される周辺機器の盗難を防止することを目的としたものである。換言すると、上記公報のコンピュータシステムは、コンピュータ本体と登録番号が一致しない周辺機器を使用不可能とするものである。すなわち、このコンピュータシステムは、コンピュータ本体を盗まれないようにしたり、情報の盗用を防ぐことを目的としてはいなかった。

#### 【0012】

本発明は係る問題に鑑みてなされたものであり、不特定多数人が利用可能な環境に設置される電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムを提供することを目的とする。

#### 【0013】

##### 【課題を解決するための手段】

上記目的を達成するため、本発明は、第1の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するためのインタフェースと、該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機

能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、インタフェースを介して接続されている外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

#### 【0014】

また、上記目的を達成するため、本発明は、第2の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するためのインタフェースと、該インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、インタフェースを介して接続されている外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報と関連する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

#### 【0015】

また、上記目的を達成するため、本発明は、第3の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする手段と、該暗証キーを記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するも

のである。

【0016】

また、上記目的を達成するため、本発明は、第4の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、記憶手段に記憶されている暗証キーの装置特定情報及び接続経路情報と一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

【0017】

また、上記目的を達成するため、本発明は、第5の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけた情報を暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

**【0018】**

また、上記目的を達成するため、本発明は、第6の態様として、自装置が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限手段と、外部装置を接続するための少なくとも二つのインタフェースと、該インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する手段と、該装置特定情報の取得元の外部装置がいずれのインタフェースを介して接続されているかを示す接続経路情報を生成する手段と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対にした情報とを関連づけて暗証キーとする手段と、該暗証キーを少なくとも一つ記憶する記憶手段と、各インタフェースを介して接続されているそれぞれの外部装置から取得した装置特定情報及び、それぞれの外部装置の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーと一致するか否かを判断する判断手段と、判断手段が一致すると判断した場合に、機能制限手段が設定する機能制限のうち装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除手段とを有する電子機器を提供するものである。

**【0019】**

上記本発明の第1から第6のいずれの態様において、外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる手段をさらに有することが好ましい。また、判断手段が判断を行ってから所定の時間が経過した後に、機能制限を再設定する手段をさらに有することが好ましい。

**【0020】**

また、上記目的を達成するため、本発明は、第7の態様として、外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、機能制限と第1の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、イン

タフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 2 の装置特定情報取得工程と、第 2 の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

#### 【0 0 2 1】

また、上記目的を達成するため、本発明は、第 8 の態様として、外部装置を接続するためのインタフェースを備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースを介して接続された外部装置から該装置を特定する装置特定情報を取得する第 1 の装置特定情報取得工程と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースを介して接続された外部装置から装置特定情報を取得する第 2 の装置特定情報取得工程と、第 2 の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーに含まれる装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第 2 の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

#### 【0 0 2 2】

また、上記目的を達成するため、本発明は、第 9 の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第 1 の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定

情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する記憶工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報の組み合わせが、記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

### 【0023】

また、上記目的を達成するため、本発明は、第10の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用を防止する方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、外部装置が、第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを組にした情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、外部装置が、第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、第2の装置特定情報取得工程において取得した装置特定情報と、第2の接続経路情報との対が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

### 【0024】

また、上記目的を達成するため、本発明は、第11の態様として、外部装置を

接続するためのインタフェースを少なくとも二つ備えた電子機器の不正使用防止方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、各機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続された外部装置から該装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行することを特徴とする電子機器の不正使用防止方法を提供するものである。

#### 【0025】

また、上記目的を達成するため、本発明は、第12の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器の不正利用防止方法であって、電子機器が、自らの機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、外部装置が、第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する第1の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、外部装置が、第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、第2の装置特定情報

取得工程において取得した装置特定情報及びこれに関する第2の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続経路情報の対と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限のうち第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを行うことを特徴とする電子機器の不正使用防止方法を提供するものである。

#### 【0026】

上記本発明の第7から第12の態様においては、第1の装置特定情報取得工程の後段に、第1の装置特定情報取得工程において電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程をさらに有することが好ましい。また、判断工程の実行後所定の時間が経過した時点で、機能制限を再設定する工程をさらに有することが好ましい。

#### 【0027】

また、上記目的を達成するため、本発明は、第13の態様として、外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、機能制限と第1の装置特定情報取得工程において取得した装置特定情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。



## 【0028】

また、上記目的を達成するため、本発明は、第14の態様として、外部装置を接続するためのインタフェースを備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器の機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、各機能制限ごとに所定の外部装置の装置特定情報とを関連づけて暗証キーとする工程と、該各暗証キーを記憶手段に記憶する工程と、インタフェースを介して電子機器に接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

## 【0029】

また、上記目的を達成するため、本発明は、第15の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する記憶工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報の組み合わせが、記憶手段に記憶されている暗証キーに含まれる装置特定情報の組み合わせと一致するか否かを判断する判断工程と、判断工

程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

#### 【0030】

また、上記目的を達成するため、本発明は、第16の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、外部装置が、第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する接続経路情報を対とした情報とを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶する工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から装置特定情報を取得する第2の装置特定情報取得工程と、外部装置が、第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、第2の装置特定情報取得工程において取得した装置特定情報と、第2の接続経路情報との対が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

#### 【0031】

また、上記目的を達成するため、本発明は、第17の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該

装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、機能制限と、一つ以上の特定の装置特定情報の組み合わせとを関連づけて暗証キーとする工程と、該暗証キーを記憶手段に記憶させる工程と、インタフェースのいずれかを介して電子機器に接続された外部装置から該装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、第2の装置特定情報取得工程において取得した装置特定情報が、記憶手段に記憶されている暗証キーと一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限工程において設定した機能制限のうち、第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

### 【0032】

また、上記目的を達成するため、本発明は、第18の態様として、外部装置を接続するためのインタフェースを少なくとも二つ備えた電子機器に内蔵され、該電子機器を制御する実質的なコンピュータに、電子機器としての機能の少なくとも一部の実行を制限して使用不可とする機能制限を一つ以上設定する機能制限工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第1の装置特定情報取得工程と、外部装置が、第1の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第1の接続経路情報を生成する第1の接続経路情報生成工程と、機能制限と、所定の装置特定情報及びこれに関する第1の接続経路情報を対にした情報とを関連づけて暗証キーとする工程と、該暗証キーを少なくとも一つ記憶手段に記憶させる工程と、インタフェースのいずれかを介して電子機器に接続されたそれぞれの外部装置から各装置を特定する装置特定情報を取得する第2の装置特定情報取得工程と、外部装置が、第2の装置特定情報取得工程においていずれのインタフェースを介して接続されたかを示す第2の接続経路情報を生成する第2の接続経路情報生成工程と、第2の装置特定情報取得工程において取得した装置特定情報及びこれに関する第2の接続経路情報との対が、記憶手段に記憶されているいずれかの暗証キーの装置特定情報及びこれに関する接続

経路情報の対と一致するか否かを判断する判断工程と、判断工程において一致すると判断した場合に、機能制限のうち第2の装置特定情報取得工程において取得した装置特定情報と装置特定情報が一致する暗証キーに関する機能制限を解除する制限解除工程とを実行させることを特徴とする電子機器の不正使用防止プログラムを提供するものである。

### 【0033】

上記本発明の第13から第18のいずれかの態様においては、電子機器を制御する実質的なコンピュータに、第1の装置特定情報取得工程において電子機器に接続された外部装置が情報記録可能な装置である場合に、該外部装置をユニークに示す情報を装置特定情報として該外部装置に記録させる工程を、第1の装置特定情報取得工程の後段においてさらに実行させることが好ましい。また、電子機器を制御する実質的なコンピュータに、判断工程の実行後所定の時間が経過した時点で、機能制限を再設定する工程をさらに実行させることが好ましい。

### 【0034】

#### 【発明の実施の形態】

##### 〔発明の概要〕

図1を用いて、本発明の概要を説明する。本発明を適用した電子機器は、その機能の少なくとも一部に制限が設定されており、制限が設定されている機能については、その制限を解除しない限り使用不能となっている。機能制限の例としては、例えば、電子機器としての機能が全く使用できなくするものであっても良いし、特定の動作（例えば、特定の情報に対するアクセス）のみが使用できなくするものであっても良い。

### 【0035】

また、本発明を適用した電子機器は、インタフェースを介して接続された外部装置をユニークに又はそれに準じて特定する機能（例えば、C I S タプルやシリアル番号を外部装置から取得する機能など）を備えている。例えば、接続された外部装置に自装置をユニークに特定する情報（M A C アドレスやシリアル番号など）が登録されている場合は、この情報を外部装置から取得することで、接続された外部装置をユニークに特定できる。また、接続された外部装置に自装置をユ

ニークに示す情報が登録されていない場合は、この装置に登録されている製造元や製品の名称を示す情報を取得することで、この装置を製品レベルや製造元レベルで特定できる。これらの情報は、既存の外部装置に予め登録されているものであり、本発明を実現するために特別な情報を外部装置に記録しておく必要はない。

さらに、外部装置が情報記録可能な装置である場合には、これをユニークに特定する情報を電子機器が書き加えるようにしてもよい。例えば、情報を記録可能な外部装置に対してフォーマット情報としてボリュームシリアル番号を記録されるようにすればよい。

#### 【0036】

これら装置をユニークに又はそれに準じて特定する情報を「装置特定情報」と定義すると、本発明における装置特定情報とは、機能に対して設定されている制限を解除するための暗証キーとして利用される情報と位置づけられる。

#### 【0037】

すなわち、特定の外部装置を示す装置特定情報を不揮発メモリなどに暗証キーとして予め記憶させておき、インタフェースを介して接続された外部装置から取得した装置特定情報が暗証キーと一致する場合に、機能に設定されている制限を解除する。

#### 【0038】

なお、図2に示すように、装置特定情報はその情報の種類によって外部装置をどの程度特定できるか（特定度）が異なる。例えば、装置特定情報がシリアル番号である場合は外部装置を1台に特定できるが、ロット番号である場合には、そのロットにおいて製造された装置のいずれかであるとししか特定できないことになる。

本発明は電子機器に上記動作を実行させることによって、電子機器の盗難や、情報の盗用の防止を図るものである。なお、図1中に破線で示すように、電子機器が上記動作の少なくとも一部を実質的なコンピュータによるソフトウェア処理で行うことも可能である。この場合は、従来と同様の構成のハードウェアを適用して本発明を実施することが可能となる。

以下、本発明の好適な実施の形態について説明する。

### 【0039】

#### 〔第1の実施形態〕

本発明を好適に実施した第1の実施形態について説明する。

図2に、本発明の第1の実施形態による不正使用防止プログラムを適用した電子機器100を示す。電子機器100は、制御部101、動作制限部102、外部装置情報取得部103、比較部104、NVRAM105、I/F106及び書込制御部107を有する。制御部101は、電子機器100が本来備える機能（例えば、演算機能、通信機能など）を実行させるための機能部である。動作制限部102は、電子機器100が本来備える機能の少なくとも一部を制御部101が実行できないように制限（機能制限）を設定したり、その制限を解除したりする。外部装置情報取得部103は、I/F106を介して接続された外部装置から装置特定情報（CISタプル、シリアル番号など）を取得する機能部である。比較部104は、NVRAM105に暗証キーとして登録されている装置特定情報と、I/F106を介して接続されている外部装置から取得した装置特定情報とを比較し、一致するか否かを判断する。NVRAM105は、電子機器の機能に設定されている制限を解除するか否かを判断する基準となる暗証キーが格納される。I/F106は、外部装置を接続するためのインタフェースであり、PCカードスロット、USBコネクタ、シリアルポート、パラレルポートなどの公知のものを適用可能である。書込制御部107は、外部装置情報取得部103が外部装置から取得した装置特定情報を基に、I/F106を介して接続されている外部装置の種類や装置特定情報が外部装置をどの程度特定する情報であるか（ユニーク、製品レベル、製造元レベルなど）を判断する。また、接続された外部装置が情報記録可能な装置であり、かつ、その装置特定情報が装置をユニークに示す情報ではない場合は、装置をユニークに示す情報を生成し、これを外部装置に記憶させる。

### 【0040】

図4に、I/F106を介して電子機器100に接続された外部装置をユニークに特定する情報を暗証キーとしてNVRAM105に登録する場合の動作の流

れを示す。

I/F 106 に外部装置が接続されると、外部装置情報取得部 103 は、接続された外部装置から装置特定情報を取得する（ステップ S101）。なお、I/F 106 に外部装置が接続されていない場合、外部装置情報取得部 103 は、外部装置が接続されていないことを示す情報を装置特定情報として取得する。書込制御部 107 は、外部装置情報取得部 103 が外部装置から取得した装置特定情報を基に、接続された外部装置が情報記録可能な装置であるか否かを判断する（ステップ S102）。

#### 【0041】

接続された外部装置が情報記録可能な装置である場合（ステップ S102/Yes）、書込制御部 107 は、外部装置情報取得部 103 が取得した装置特定情報が装置をユニークに示す情報であるか否かを判断する（ステップ S103）。装置特定情報が装置をユニークに示す情報ではない場合（ステップ S103/No）、書込制御部 107 は、装置をユニークに示す情報を生成し（ステップ S104）、これを外部装置に記録させる（ステップ S105）。これにより、これ以降に外部装置情報取得部 103 がこの外部装置から装置特定情報を取得する場合は、ステップ S105 で書き込んだ情報が装置特定情報として取得されることになる。その後、書込制御部 107 は、外部装置に記録させた情報と同じ情報を NVRAM 105 に出力し、機能制限を解除するための暗証キーとして登録する（ステップ S106）。

#### 【0042】

一方、I/F 106 を介して接続された外部装置が情報記録可能な装置でない場合や（ステップ S102/No）、外部装置から取得した装置特定情報が装置をユニークに示す情報である場合（ステップ S103/Yes）、書き込み制御部 107 は、外部装置情報取得部 103 が外部装置から取得した装置特定情報をそのまま NVRAM 105 へ出力し、機能制限を解除するための暗証キーとして登録する（ステップ S106）。

#### 【0043】

図 5 に、電子機器の機能に設定されている制限を I/F 106 を介して接続し

た外部装置を用いて解除する際の動作の流れを示す。

I/F 106 に外部装置が接続されると、外部装置情報取得部 103 は、接続された外部装置から装置特定情報を取得する（ステップ S 201）。比較部 104 は、現在 I/F 106 に接続されている外部装置の装置特定情報を外部装置情報取得部 103 から取得するとともに、NVRAM 105 に暗証キーとして登録されている装置特定情報を読み出す（ステップ S 202）。比較部 104 は、これらの情報を比較し、一致するか否かを判断する（ステップ S 203）。

#### 【0044】

比較結果が一致する場合（ステップ S 203 / Yes）、比較部 104 は動作制限部 102 に指示を送り、動作制限部 102 が制御部 101 に対して設定している制限を解除し、制限されていた機能を使用できるようにする（ステップ S 204）。

一方、比較結果が一致しない場合は（ステップ S 203 / No）、制御部 101 に対して設定されている制限を解除しない。

#### 【0045】

このように、機能制限を解除する動作を一度だけ実行する場合は、機能制限を解除する際に暗証キーとなる外部装置が接続されていればよく、機能制限を解除した後に暗証キーとなる外部装置を取り外しても電子機器 100 は使用可能となる。このため、使用頻度の低い外部装置を暗証キーとして NVRAM 105 に登録した場合には、機能制限を解除した後にその外部装置を取り外し、I/F 106 に別の外部装置を接続して使用することが可能となる。

#### 【0046】

また、機能制限を解除する動作を定期的に行うようにしてもよい。図 6 に、この場合の電子機器 100 の動作の流れを示す。

ステップ S 201' ~ S 204' の動作は、図 5 のステップ S 201 ~ S 204 の動作と同様である。

ステップ S 203' の処理終了後所定の時間が経過すると（ステップ S 205' / Yes）、動作制限部 102 は、ステップ S 204' において解除した制限を再び制御部 101 に対して設定し、機能制限に係る機能を使用できない状態に



する（ステップ S206）。

その後、ステップ S201' に戻り、比較部 104 は、現在 I/F106 を介して接続されている外部装置から装置特定情報取得部 103 が取得した装置特定情報と、NVRAM105 に暗証キーとして登録されている情報とを比較して、機能制限を解除するか否かを決定する（ステップ S201' ～ S203'）。

#### 【0047】

機能制限を解除する動作を定期的に行う場合は、一度機能制限を解除しても、所定時間経過後に暗証キーとして NVRAM105 に登録されている外部装置が I/F106 を介して接続されているか否かを比較部 104 が再度判断するため、セキュリティ性を高めることが可能となる。

例えば、機能制限が解除された状態の電子機器 100 を盗んだとしても、暗証キーとして NVRAM105 に登録された外部装置を所持していなければ、所定時間経過後に電子機器 100 を使用できなくなるため、電子機器 100 の盗難を抑止できる。

#### 【0048】

また、機能制限を再設定するまでの時間を短くすれば、暗証キーとして NVRAM105 に登録されている外部装置が I/F106 を介して接続されていない限り電子機器 100 を使用不能にできる。

例えば、I/F106 を介して接続された外部装置から取得した装置特定情報を NVRAM105 に暗証キーとして登録された情報と比較してから、機能制限を再設定するまでの間隔を 1/100 秒とすれば、実質的には、暗証キーとして登録された外部装置が接続されていない状態で電子機器 100 を使用することは不可能となる。

#### 【0049】

このように、電子機器 100 は、機能制限を解除する動作を一度だけ行っても良いし、繰り返し行ってもよい。

換言すると、電子機器 100 には、暗証キーとして登録された外部装置を利用開始時（機能制限解除時）のみ接続し、その後は接続を継続する必要のない利用形態と、利用期間中継続して接続しておく必要がある利用形態とがある。電子機

器 100 をどちらの利用形態で利用するかは、電子機器 100 が適用されるシステムの性格に応じて選択又は切り替えることが可能である。

#### 【0050】

本実施形態では、接続された外部装置から装置特定情報を取得する機能を備えた電子機器に対して、電子機器としての機能の少なくとも一部を実行できないように制限を施しておくとともに、特定の外部装置が接続されていること（すなわち、接続された外部装置から特定の装置特定情報を取得した場合）を制限を解除する条件として予め登録しておく。これにより、機能の制限を解除する条件として予め登録されている外部装置が接続された場合のみ、又は、接続されている場合のみ制限が施されている機能を利用することが可能となる。

#### 【0051】

##### 〔第2の実施形態〕

本発明を好適に実施した第2の実施形態について説明する。

図7に、本実施形態による不正使用防止プログラムを適用した電子機器200を示す。電子機器200は、I/F106を複数（106a、106b）備える他は、第1の実施形態の電子機器100と同様である。

#### 【0052】

本実施形態においては、装置特定情報が単独で、又は、二つの装置特定情報を組としたものが機能制限を解除するための暗証キーとして用いられる。

#### 【0053】

図8に、NVRAM105に暗号キーとして二つの装置特定情報からなる組を登録する場合の動作の流れを示す。

I/F106a及び106bのそれぞれに外部装置が接続されると、電子機器200は、第1の実施形態のステップS301～S305と同様の処理を、I/F106aや106bを介して接続された外部装置のそれぞれについて別個に行う（ステップS301a～S305a、ステップS301b～S305b）。

その後、書込制御部107は、I/F106a及び106bのそれぞれを介して接続されている外部装置について、装置特定情報、又は、外部装置に記録させた情報と同じ情報を、暗証キーとしてNVRAM105に登録する（ステップS

306)。

#### 【0054】

図9に、NVRAM105に暗号キーとして二つの装置特定情報からなる組を登録した場合に、I/F106a及び106bのそれぞれを介して接続した外部装置を用いて電子機器の機能に設定されている制限を解除する動作の流れを示す。

#### 【0055】

I/F106a及び106bのそれぞれに外部装置が接続されると、外部装置情報取得部103は、それぞれの外部装置から装置特定情報を取得する(ステップS401a、S401b)。なお、I/F106aや106bに外部装置が接続されていない場合、外部装置情報取得部103は、外部装置が接続されていないことを示す情報を装置特定情報として取得する。比較部104は、現在I/F106a、106bにそれぞれ接続されている外部装置の装置特定情報を外部装置情報取得部103から取得するとともに、NVRAM105に暗証キーとして登録されている装置特定情報の組を読み出す(ステップS402)。さらに比較部104は、現在I/F106a及び106bを介して接続されている外部装置の組合せ(すなわち、装置特定情報の組合せ)が、暗証キーとして登録されている装置特定情報の組合せと一致するか否かを判断する(ステップS403)。

#### 【0056】

比較結果が一致する場合(ステップS403/Yes)、比較部104は動作制限部102に指示を送り、動作制限部102が制御部101に対して設定している制限を解除し、制限されていた機能を使用できるようにする(ステップS404)。

一方、比較結果が一致しない場合(ステップS403/No)、動作制限部102は、特定の機能の制限を引き続いて行う。

#### 【0057】

図10に、NVRAM105に暗号キーとして一つの装置特定情報を単独で登録した場合に、I/F106a及び106bのそれぞれを介して接続した外部装置を用いて、制限されている電子機器の機能を復帰させる動作の流れを示す。

## 【0058】

I/F106a及び106bの少なくともいずれかに外部装置が接続されると、外部装置情報取得部103は、それぞれの外部装置から装置特定情報を取得する（ステップS501a、S501b）。なお、I/F106aや106bに外部装置が接続されていない場合、外部装置情報取得部103は、外部装置が接続されていない旨を示す情報を装置特定情報として取得する。比較部104は、現在I/F106aに接続されている外部装置の装置特定情報を外部装置情報取得部103から取得するとともに、NVRAM105に暗証キーとして登録されている装置特定情報を読み出す（ステップS502）。さらに比較部104は、現在I/F106a又は106bに接続されているいずれかの外部装置の装置特定情報と、機能制限を解除するための暗証キーとして登録されている装置特定情報とを比較し、一致するか否かを判断する（ステップS503）。

## 【0059】

比較結果が一致する場合（ステップS503／Yes）、比較部104は動作制限部に指示を送り、動作制限部102が制御部101に対して設定している制限を解除し、制限されていた機能を使用できるようにする。

一方、比較結果が一致しない場合、（ステップS503／No）、動作制限部102は、特定の機能の制限を引き続いて行う。

## 【0060】

なお、ここでは電子機器がI/F106を二つ（106a及び106b）備える場合を例に説明を行ったが、I/F106を三つ以上備えていてもよい。例えば、I/F106を三つ備える場合は、NVRAM105には、三つの装置特定情報の組合せ、二つの装置特定情報の組合せ、及び、一つの装置特定情報を単独で暗証キーとして登録することが可能となる。

すなわち、I/F106をn個（nは3以上の自然数）備える場合は、NVRAM105にはn個～2個の装置特定情報の組合せ、又は装置特定情報を単独で暗証キーとして登録することが可能となる。

また、本実施形態においても機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第1の実施形態と同様に、装置特定情報と暗証キーと

の比較を行った後所定の時間が経過した時点で機能制限を再設定し、再び装置特定情報と暗証キーとの比較を行う処理となるため説明は省略する。

#### 【0061】

このように、本実施形態では、接続された外部装置から装置特定情報を取得する機能を備えた電子機器に対して、電子機器としての機能の少なくとも一部を実行できないように制限を施しておくとともに、特定の外部装置が接続されていること（すなわち、接続された外部装置から特定の装置特定情報を取得した場合）を制限を解除する条件として予め登録しておく。これにより、機能の制限を解除する条件として予め登録されている外部装置が接続された場合のみ、又は、接続されている場合のみ制限が施されている機能を利用することが可能となる。

また、電子機器の機能の制限を解除する条件として、複数の外部装置の組合せを予め登録しておけば、この組合せに係る外部装置が全て接続されている場合のみ、制限が施されている機能を利用することなどが可能となる。

#### 【0062】

##### 〔第3の実施形態〕

本発明を好適に実施した第3の実施形態について説明する。

図11に、本実施形態による不正使用防止プログラムを適用した電子機器300を示す。電子機器300は、I/F106及び外部装置情報取得部103を二つずつ備える他は、第2の実施形態による電子機器200と同様である。

外部装置情報取得部103aは、I/F106aを介して接続された外部装置から装置特定情報を取得する。また、外部装置情報取得部103bは、I/F106bを介して接続された外部装置から装置特定情報を取得する。外部装置情報取得部103a、103bが取得した装置特定情報は、第2の実施形態と同様に、暗証キーとしてNVRAM105に格納されたり、機能制限を解除するか否かを判断するために用いられる。

#### 【0063】

図12に、NVRAM105に暗号キーとして二つの装置特定情報からなる組を登録する場合の動作の流れを示す。

ステップS601a～S605a、及び、ステップS601b～S605bの

動作は、第2の実施形態のステップS301～S305a、ステップS301b～S305bとそれぞれ同様である。

ステップS606において、書込制御部107は、I/F106a及び106bのそれぞれを介して接続されている外部装置について、装置特定情報、又は、外部装置に記録させた情報と同じ情報を、暗証キーとしてNVRAM105に登録する。

#### 【0064】

本実施形態においては、I/F106a及び106bのそれぞれを介して接続されている外部装置からの装置特定情報は、各々が別個の伝送路を経て書込制御部107へ入力される。このため、書込制御部107においては、外部装置情報取得部103a及び103bが取得した装置特定情報はそれぞれ別個に扱われる。これにより、電子機器300は、同一の外部装置であっても、I/F106aを介して接続された場合と、I/F106bを介して接続された場合とを区別することができる。

図13に、書込制御部107がNVRAM105に登録する暗証キーの一例を示す。同図に示すように、本実施形態においては、どの外部装置が接続されているかだけでなく、その外部装置がどのインタフェースを介して接続されているかをも含めた条件を機能制限を解除するための暗証キーとして登録することが可能となる。

#### 【0065】

図14に、NVRAM105に暗号キーとして二つの装置特定情報からなる組に登録した場合に、I/F106a及び106bのそれぞれを介して接続した外部装置を用いて電子機器の機能に設定されている制限を解除する動作の流れを示す。

#### 【0066】

I/F106a及び106bのそれぞれに外部装置が接続されると、外部装置情報取得部103a及び103bは、それぞれの外部装置から装置特定情報を取得する（ステップS701a、S701b）。なお、I/F106aや106bに外部装置が接続されていない場合、外部装置情報取得部103aや103bは

、外部装置が接続されていないことを示す情報を装置特定情報として取得する。比較部104は、現在I/F106a、106bにそれぞれ接続されている外部装置の装置特定情報を外部装置情報取得部103a及び103bから取得するとともに、NVRAM105に暗証キーとして登録されている装置特定情報の組を読み出す（ステップS702）。さらに比較部104は、現在I/F106a及び106bを介して接続されている外部装置の組合せ（すなわち、装置特定情報の組合せ）が、暗証キーとして登録されている装置特定情報の組合せと一致するか否かを判断する（ステップS703）。

#### 【0067】

比較結果が一致する場合（ステップS703／Yes）、比較部104は、現在接続されている各外部装置が、装置特定情報を暗証キーとして登録した時と同じインタフェースを介して接続されているか否かを判断する（ステップS704）。同じインタフェースを介して接続されている場合は（ステップS704／Yes）、比較部104は動作制限部102に指示を送り、動作制限部102が制御部101に対して設定している制限を解除し、制限されていた機能を使用できるようにする（ステップS705）。

#### 【0068】

現在I/F106a及び106bを介して接続されている外部装置から取得した装置特定情報の組合せが、暗証キーとしてNVRAM105に登録されている装置特定情報の組合せと一致しない場合（ステップS703／No）、又は、装置特定情報を暗証キーとして登録した時と異なるインタフェースを介して接続されている場合（ステップS704／No）、動作制限部102は、特定の機能の制限を引き続いて行う。

#### 【0069】

このように、本実施形態においては、電子機器は外部装置がどのインタフェースを介して接続されているかを区別できる。これにより、例えば、I/F106aを介して接続された外部装置Aから取得した装置特定情報と、I/F106bを介して接続された外部装置Bから取得した装置特定情報との組み合わせがNVRAM105に暗証キーとして登録されている場合は、I/F106aを介して

外部装置Bを接続し、I/F106bを介して外部装置Aを接続しても、機能の制限を解除することはできない。

すなわち、本実施形態では、電子機器の盗難を抑止したり、情報の盗用を防止したりする効果を第2の実施形態よりも高いレベルで得ることができる。

#### 【0070】

なお、第2の実施形態と同様に、ここでは電子機器がI/F106を二つ（106a及び106b）備える場合を例に説明を行ったが、I/F106を三つ以上備えていてもよい。I/F106を三つ備える場合は、NVRAM105には、三つの装置特定情報の組合せ、二つの装置特定情報の組合せ、及び、一つの装置特定情報を単独で暗証キーとして登録することが可能となる。

すなわち、I/F106をn個（nは3以上の自然数）備える場合は、NVRAM105にはn個～2個の装置特定情報の組合せ、又は装置特定情報を単独で暗証キーとして登録することが可能となる。

また、本実施形態においても機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第1の実施形態と同様に、装置特定情報と暗証キーとの比較を行った後所定の時間が経過した時点で機能制限を再設定し、再び装置特定情報と暗証キーとを比較する処理となるため、説明は省略する。

#### 【0071】

本実施形態において、電子機器300のNVRAM105には、外部装置から取得した装置特定情報に加えて、外部装置がどのインタフェースを介して接続されているかを暗証キーとして登録できる。このため、機能制限を解除するためのキーとなる外部装置が電子機器300と共に盗まれたとしても、暗証キーを登録した時と同一のインタフェースを介して電子機器300に接続されなければ、電子機器300に設定されている機能制限は解除されない。これにより、機能制限を解除する条件を知らない者が電子機器300を不正に使用したり、情報を盗用することは困難となるため、電子機器300が盗まれたり、情報が盗用されることを防止できる。

#### 【0072】

〔第4の実施形態〕



本発明を好適に実施した第4の実施形態について説明する。本実施形態においては、電子機器に機能制限が多段階に分けて設定されており、接続された外部装置から取得した装置特定情報に応じて制限を解除する程度を変更する。

#### 【0073】

本実施形態においては、第1の実施形態と同様の電子機器を適用できる。電子機器に対して設定される機能制限は、NVRAM105に機能制限テーブルとして登録される。図15に、この一例を示す。

#### 【0074】

「利用可能機能」は、電子機器100の機能のうちどの機能が利用可能とすることを示しており、“Nothing”は全ての機能が利用不可とすることを、“Read”は、データの読み出しを可能とすることを、“Write”はデータの書込を可能とすることを、“All”はシステムの設定を含めて全ての機能を利用可能とすることを示している。

「暗証キー」は、機能制限を解除する条件を示しており、“A”、“B”、“C”は、I/F106を介して“外部装置A”、“外部装置B”、“外部装置C”が接続されることをそれぞれ示している。なお、“Default”は、初期状態（常態）を示す。

#### 【0075】

図16に、上記条件がNVRAM105に機能制限テーブルとして登録されている電子機器において、電子機器に設定されている機能制限をI/F106に接続された外部装置を用いて解除する場合の動作の流れを示す。

I/F106を介して外部装置が接続されると、外部装置情報取得部103は、接続された外部装置から装置特定情報を取得する（ステップS801）。比較部104は、外部装置情報取得部103から現在I/F106を介して接続されている外部装置の装置特定情報を取得するとともに、NVRAM105から機能制限テーブルを読み出す。比較部104は、機能制限テーブルに暗証キーとして登録されている装置特定情報の中に、外部装置情報取得部103から取得した装置特定情報があるか否かを判定する（ステップS802）。

#### 【0076】

外部装置情報取得部 103 から取得した装置特定情報が “A” であった場合、すなわち、I/F 106 を介して外部装置 A が接続されている場合（ステップ S802/A）、動作制限部 102 は、制御部 101 に対して設定している制限を全て解除して、電子機器 100 の機能を全て使用可能とする（ステップ S803）。

#### 【0077】

外部装置情報取得部 103 から取得した装置特定情報が “B” であった場合、すなわち、I/F 106 を介して外部装置 B が接続されている場合（ステップ S802/B）、動作制限部 102 は、制御部 101 に対して設定している制限のうち、情報の書き込み・読み出しに関する機能の制限のみを解除する（ステップ S804）。

#### 【0078】

外部装置情報取得部 103 から取得した装置特定情報が “C” であった場合、すなわち、I/F 106 を介して外部装置 C が接続されている場合（ステップ S802/C）、動作制限部 102 は、制御部 101 に対して設定している制限のうち、情報の読み出しに関する機能の制限のみを解除する（ステップ S805）。

#### 【0079】

外部装置情報取得部 103 から取得した装置特定情報が “A”、“B” 及び “C” のいずれでもない場合、又は、外部装置情報取得部 103 から取得した装置特定情報が、外部装置が接続されていないことを示している場合（ステップ S802/その他）、動作制限部 102 は、制御部 101 に対して設定している制限をいずれも解除せず、全ての機能を使用不可とする状態を継続させる（ステップ S806）。

#### 【0080】

本実施形態の電子機器 100 の動作について具体的な例を挙げて説明する。ここでは、電子機器 100 を用いたシステムを管理する「システム管理者 A」、常時システムを利用する「利用者 B」、一時的にシステムを利用する「利用者 C」及び「利用者 D」、システムの使用する権限がない「部外者 E」が存在するもの

とする。

#### 【0081】

システム管理者Aは、NVRAM105に外部装置A、B及びCを暗証キーとして上記同様の機能制限を設定しておく。登録後、外部装置Aは自身が所持し、外部装置Bは利用者Bに手渡す。また、外部装置Cは一時利用者用に貸し出す準備をしておく。

#### 【0082】

常態においてはシステムの全ての機能に制限が設定されているため、システムを利用しようとする各人は、手持ちの外部装置を用いて、機能制限を解除しなければならない。

例えば、利用者Bがシステムを使用する場合は、自身に割り当てられた外部装置Bを用いて機能制限を解除する。また、利用者Cがシステムを使用したい場合は、システム管理者Aに許可を得て外部装置Cを借用し、機能制限を解除した上で使用システムを使用し、使用後に外部装置Bを返却する。利用者Dがシステムを使用する場合は、利用者Cと同様である。

部外者Eが不正に（管理者Aの許可を得ずに）システムを使用しようとした場合は、機能制限を解除できないため、システムを使用することはできない。

#### 【0083】

なお、ここでは、電子機器100がインタフェースとしてI/F106を一つだけ備える場合を例に説明を行ったが、第2の実施形態や第3の実施形態と同様に、電子機器100はI/F106を複数備えていても良い。

#### 【0084】

このように、本実施形態によれば、電子機器の盗難や情報の盗用を抑止できるとともに、多段階に設定された機能制限を電子機器に接続された外部装置の種類に応じて解除することで、多段階のセキュリティーを電子機器に設定できる。

本実施形態においても、機能制限を解除する動作を繰り返し実行するようにしてもよい。この場合は第1の実施形態と同様に、外部装置から取得した装置特定情報と暗証キーとを比較した後所定の時間が経過した時点で機能制限を再設定し、再び外部装置から取得した装置特定情報と暗証キーとを比較する処理であるた

め説明は省略する。

#### 【0085】

なお、上記各実施形態は、本発明の好適な実施の一例であり、本発明はこれに限定されるものではない。

例えば、上記実施形態では外部装置情報取得部 103 が情報記録可能な外部装置から取得した装置特定情報が装置をユニークに示すものでない場合に、この装置に対して装置をユニークに示す情報を付与しているが、本発明はこれに限定されるものではない。

#### 【0086】

また、上記各実施形態においては、暗証キーを NVRAM 105 に格納しているが、情報を不揮発に保存できればどのような記憶装置を用いても構わない。例えば、情報量が多い場合には、ハードディスクドライブのような容量の大きい記憶装置を用いてもよい。

#### 【0087】

さらに、上記各実施形態における暗証キーや制限テーブルのデータ構造は、あくまでも一例であり、これに限定されるものではない。

このように、本発明は様々な変形が可能である。

#### 【0088】

##### 【発明の効果】

以上の説明によって明らかなように、本発明によれば、不特定多数人が利用可能な環境に設置された電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正使用防止方法並びにその不正使用防止プログラムを提供できる。

##### 【図面の簡単な説明】

#### 【図 1】

本発明の概要を説明するための図である。

#### 【図 2】

装置特定情報の種類の及びその特定度の関係の一例を示す図である。

#### 【図 3】

本発明を好適に実施した第 1 の実施形態に係る電子機器の構成を示す図である。

。

【図 4】

第 1 の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れの一例を示す図である。

【図 5】

第 1 の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図 6】

第 1 の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの別の一例を示す図である。

【図 7】

本発明を好適に実施した第 2 の実施形態に係る電子機器の構成を示す図である。

。

【図 8】

第 2 の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れの一例を示す図である。

【図 9】

第 2 の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図 10】

第 2 の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

【図 11】

本発明を好適に実施した第 3 の実施形態に係る電子機器の構成を示す図である。

。

【図 12】

第 3 の実施形態に係る電子機器が暗証キーを登録する場合の動作の流れを示す図である。

## 【図 13】

第3の実施形態における暗証キーの一例を示す図である。

## 【図 14】

第3の実施形態に係る電子機器が機能制限を解除する場合の動作の流れの一例を示す図である。

## 【図 15】

機能制限テーブルの一例を示す図である。

## 【図 16】

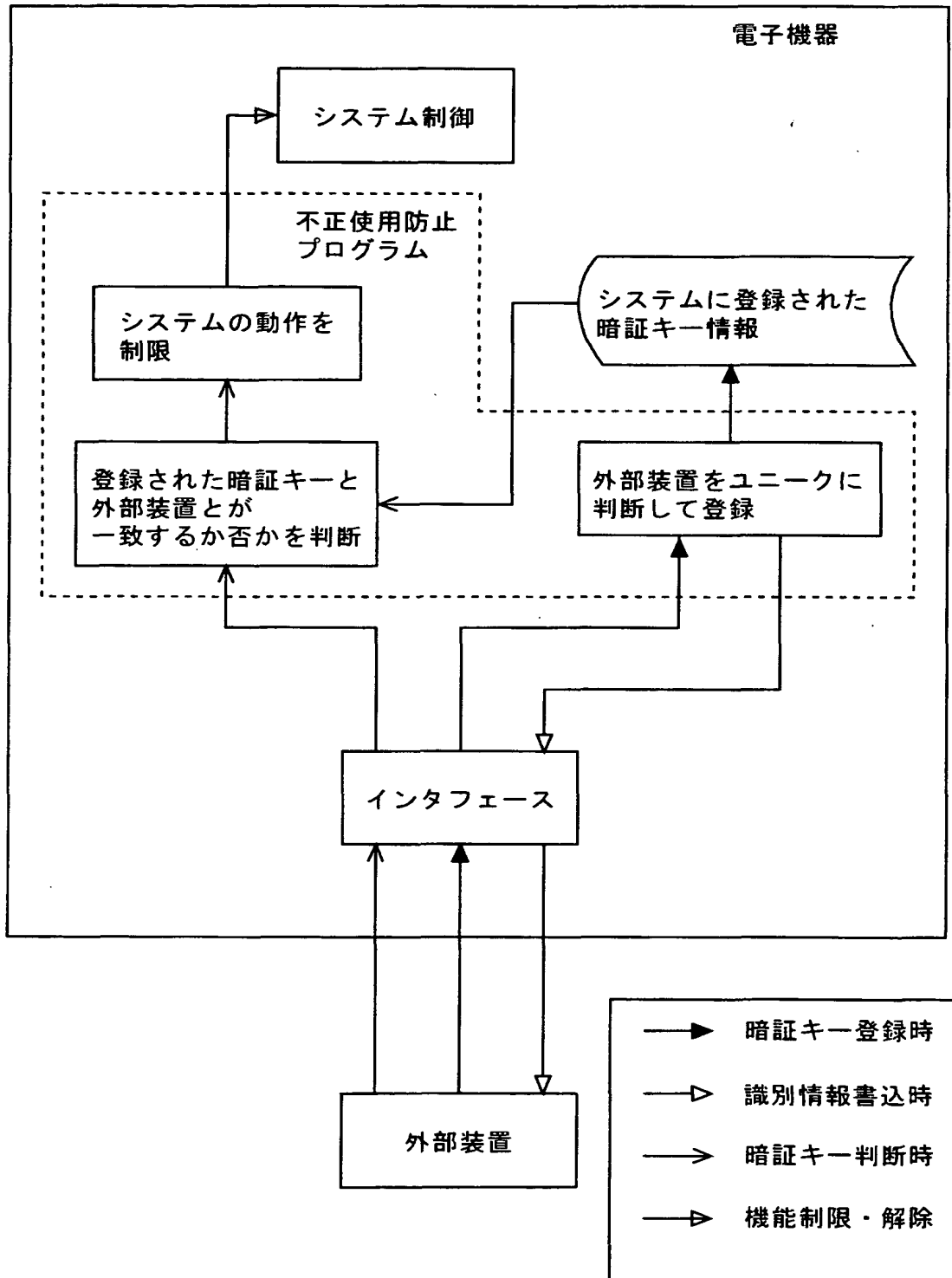
本発明を好適に実施した第4の実施形態に係る電子機器が機能制限解除する場合の動作の流れの一例を示す図である。

## 【符号の説明】

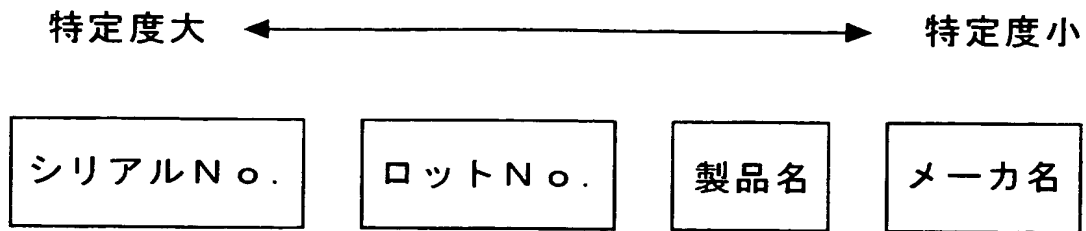
- 100、200、300 電子機器
- 101 制御部
- 102 動作制限部
- 103、103a、103b 外部装置情報取得部
- 104 比較部
- 105 NVRAM
- 106、106a、106b インタフェース (I/F)
- 107 書込制御部

【書類名】 図面

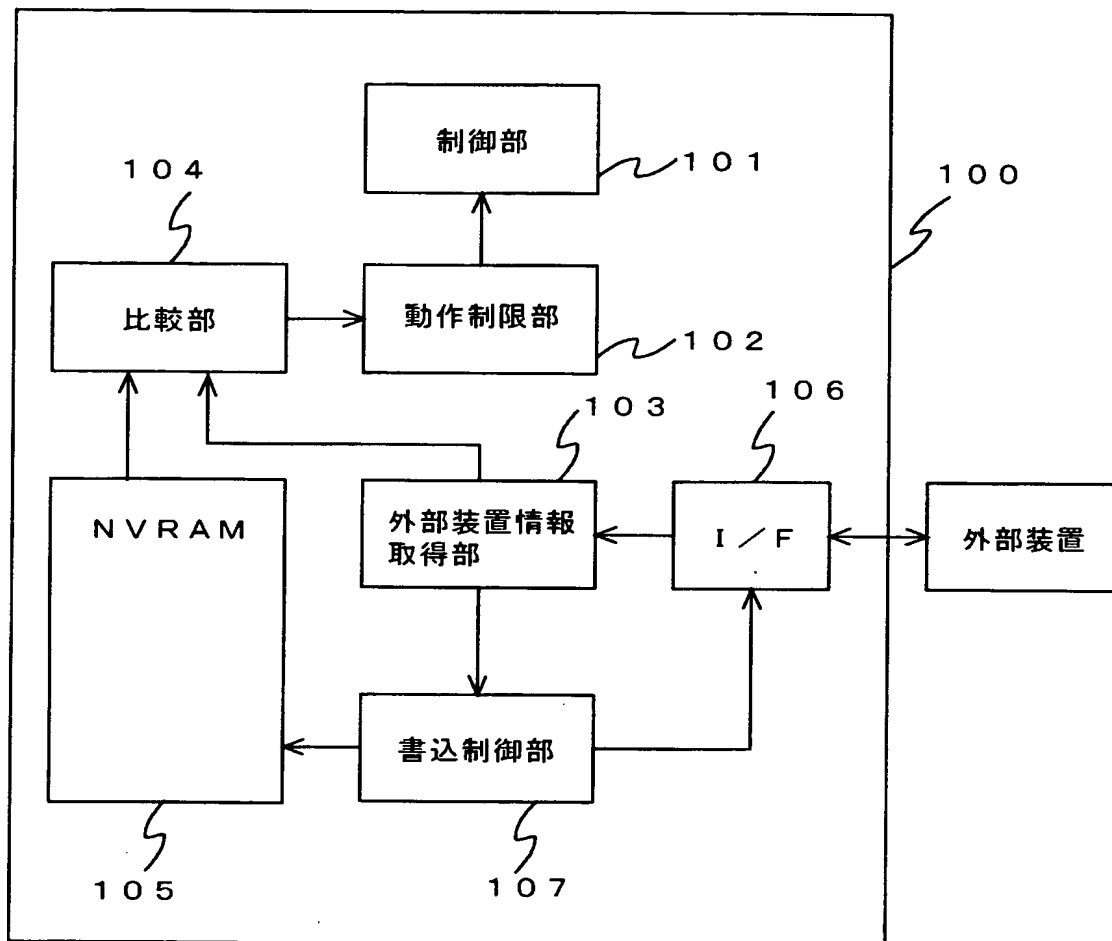
【図 1】



【図 2】

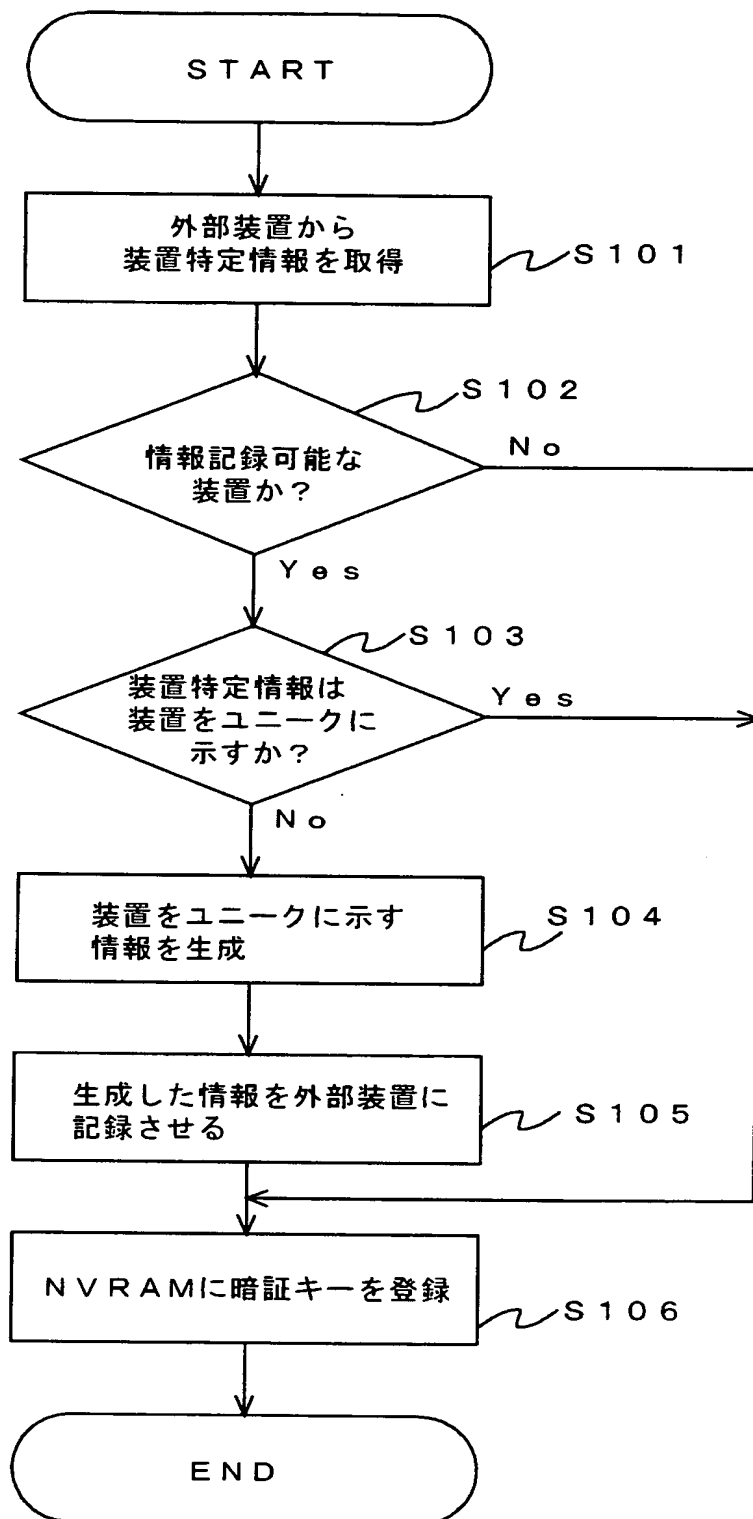


【図 3】

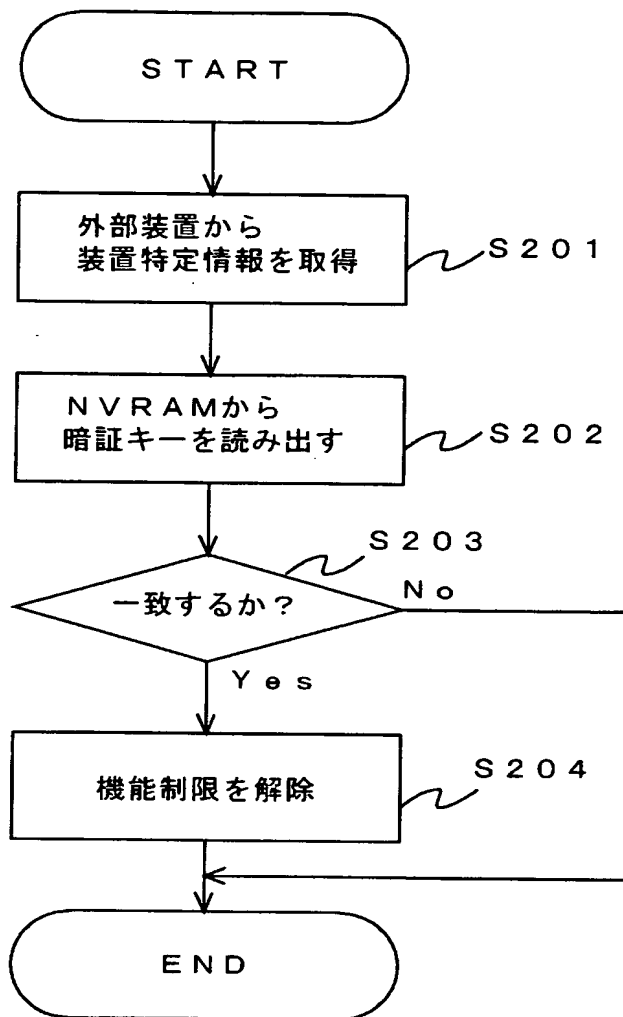




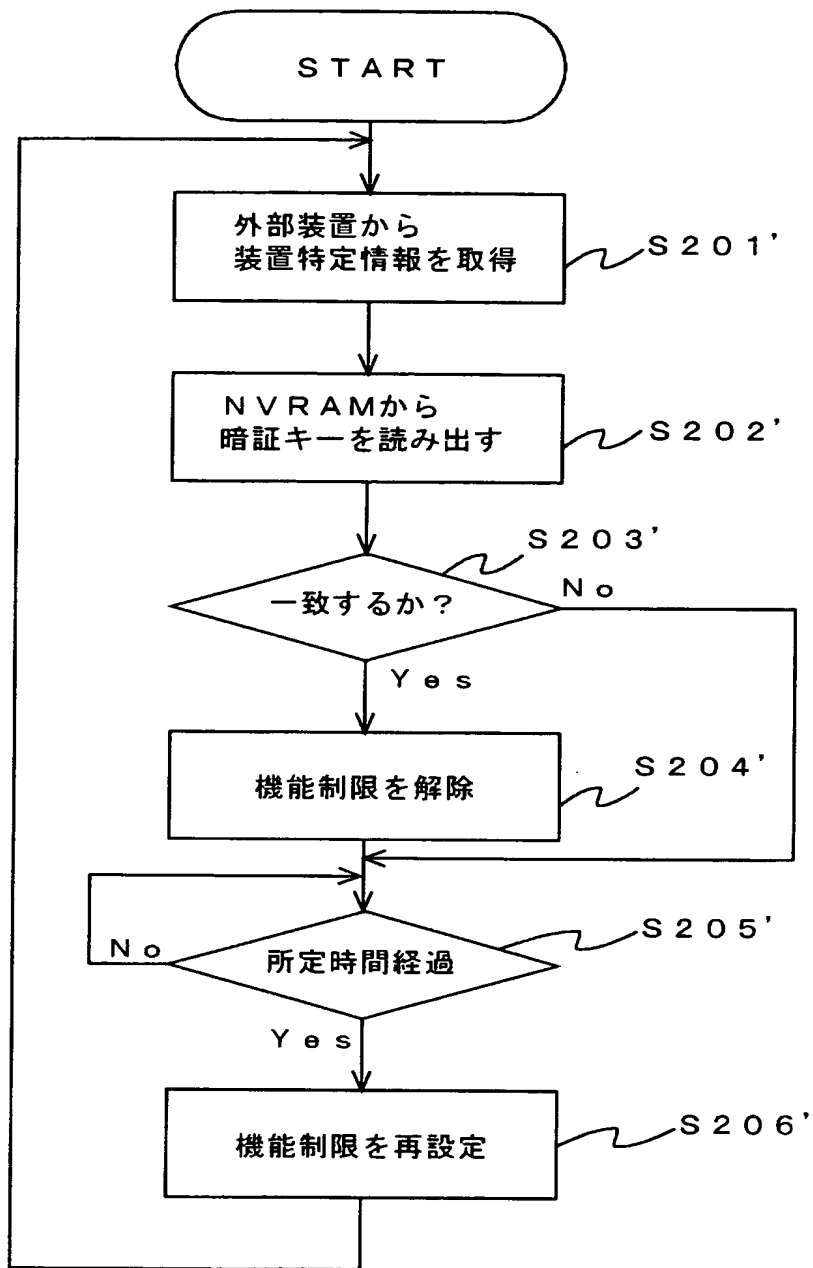
【図4】



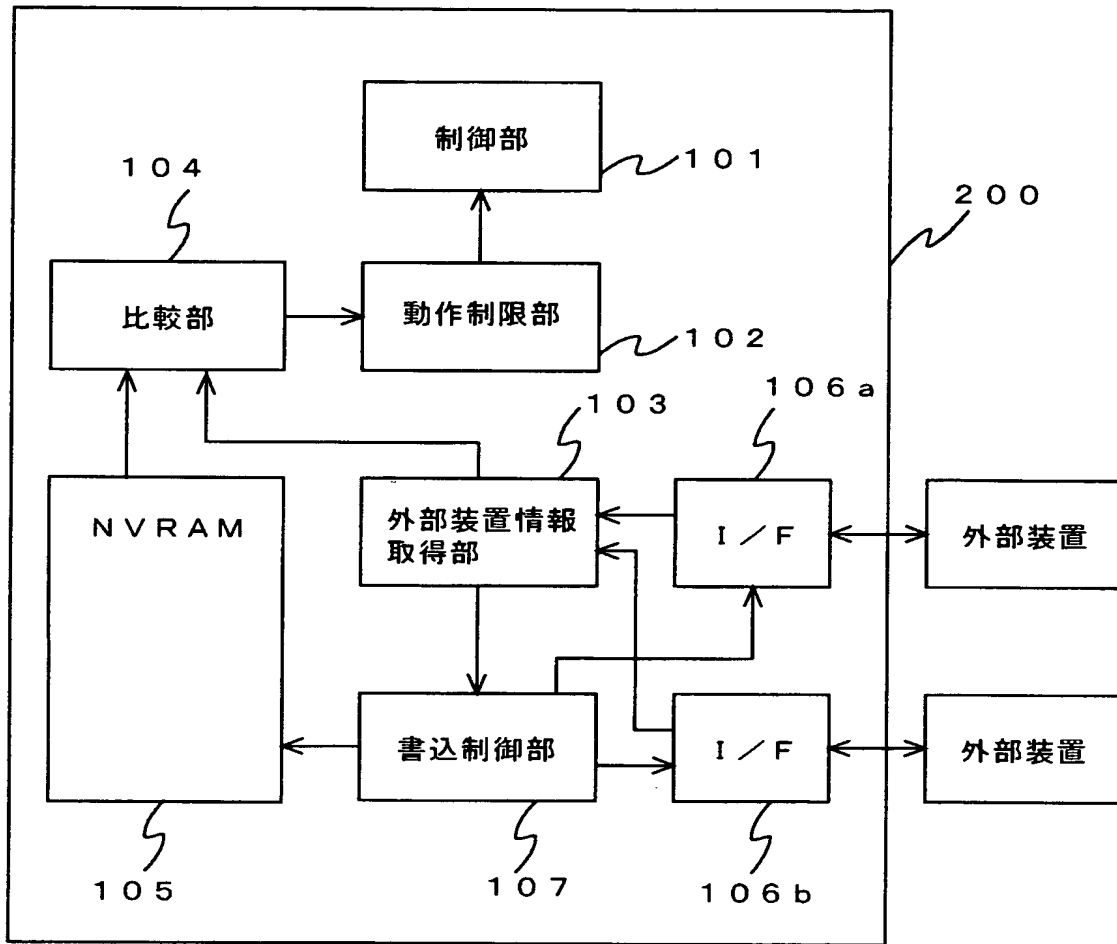
【図 5】



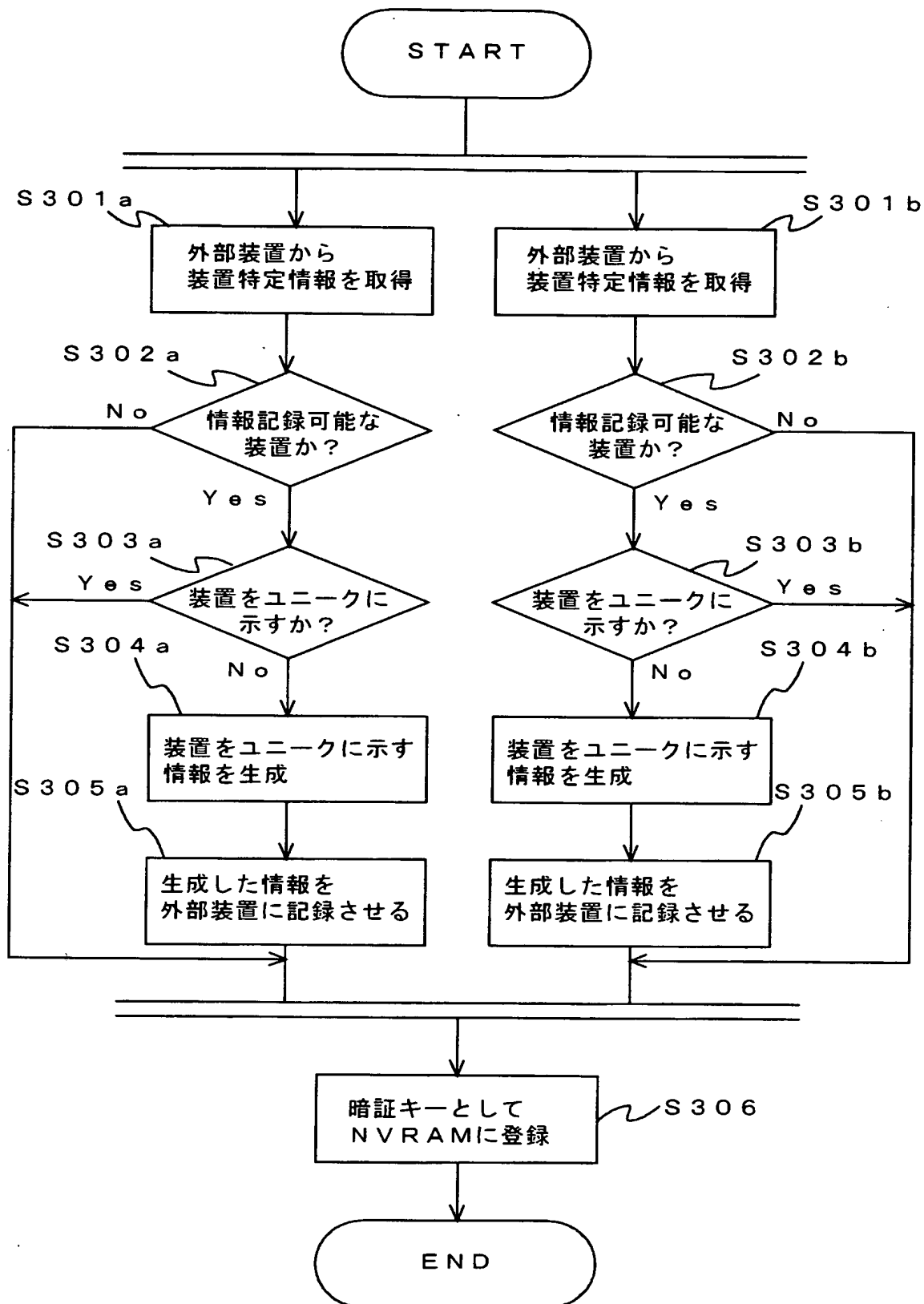
【図 6】



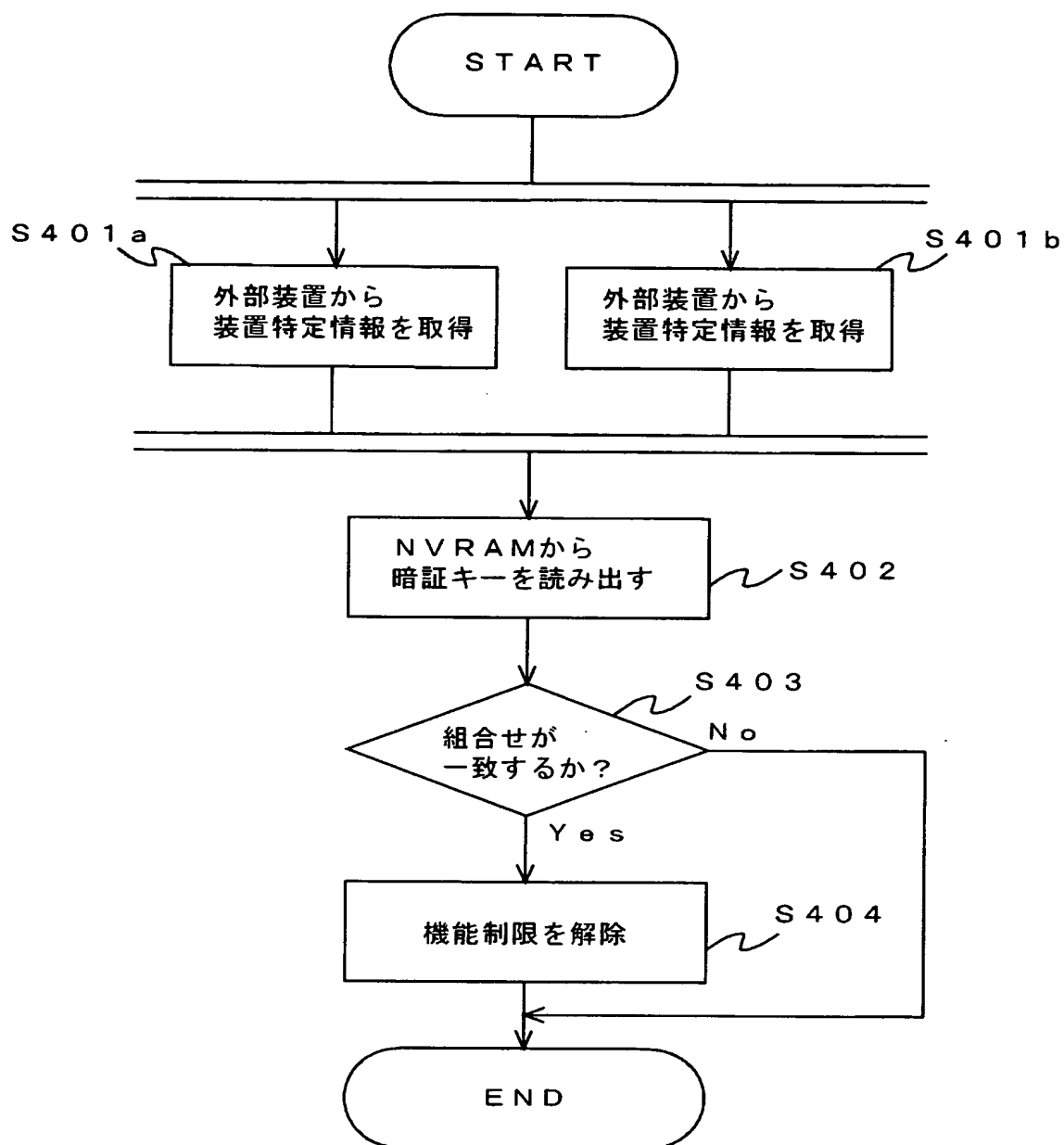
【図 7】



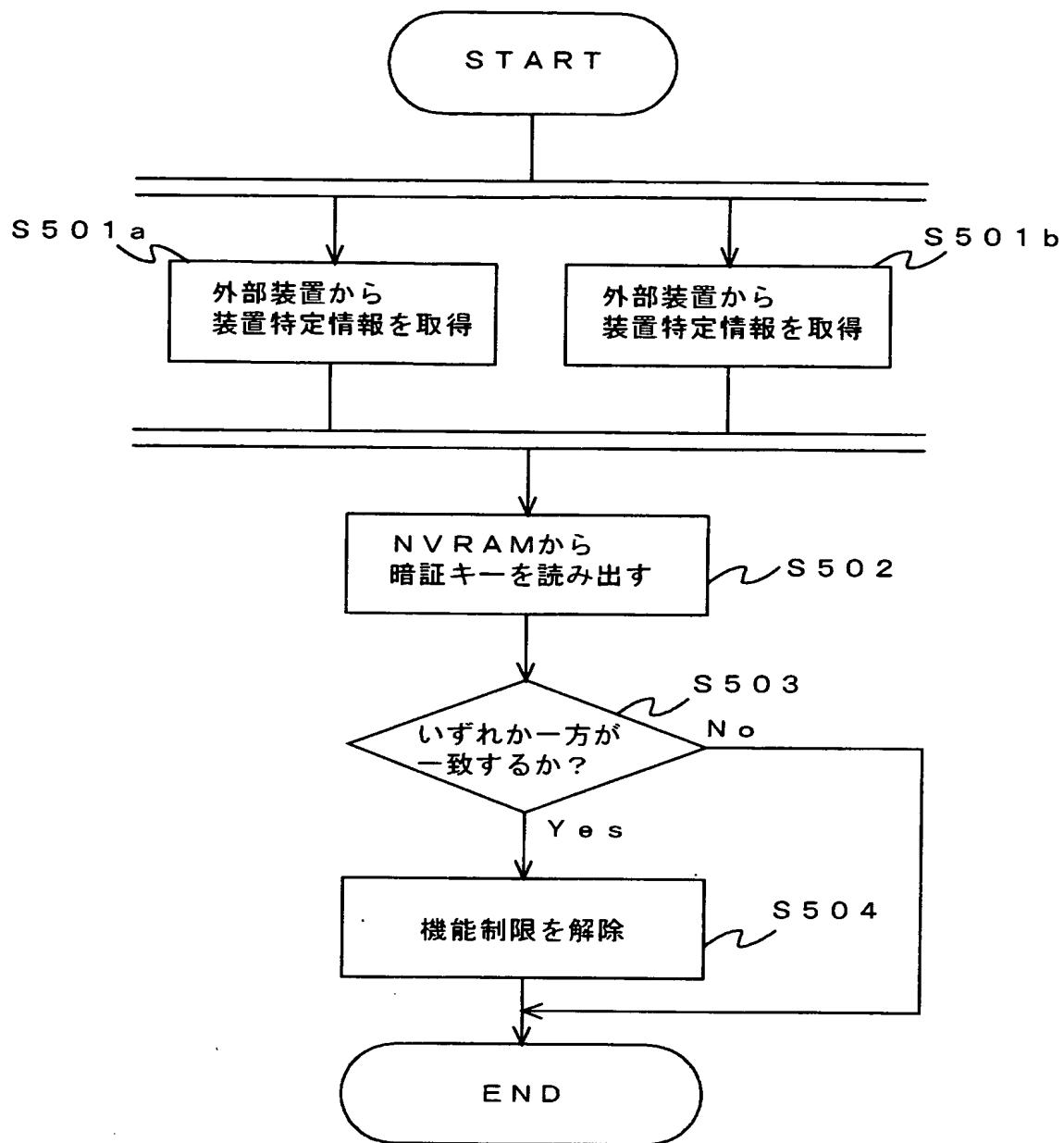
【図8】



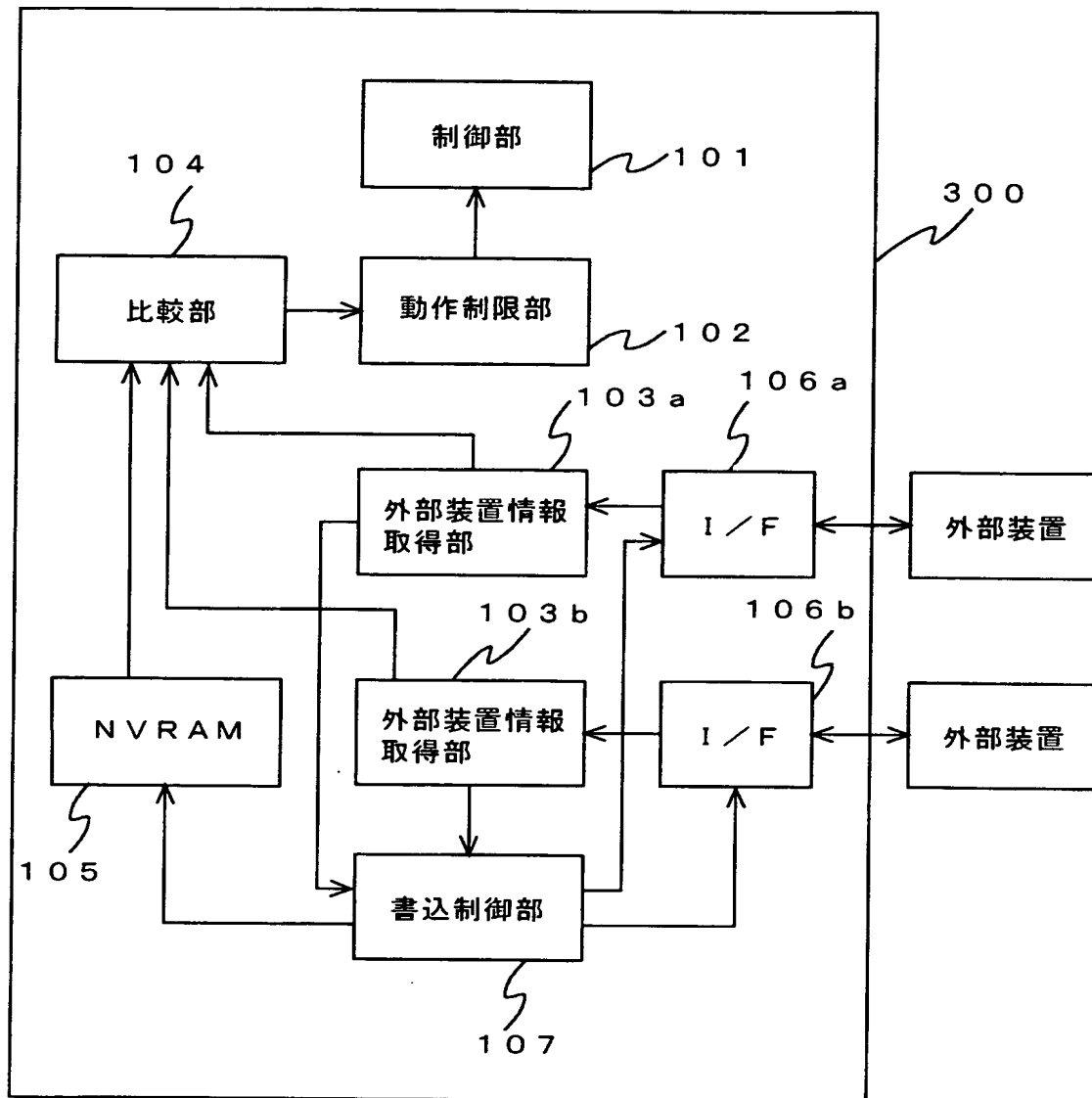
【図9】



【図 10】

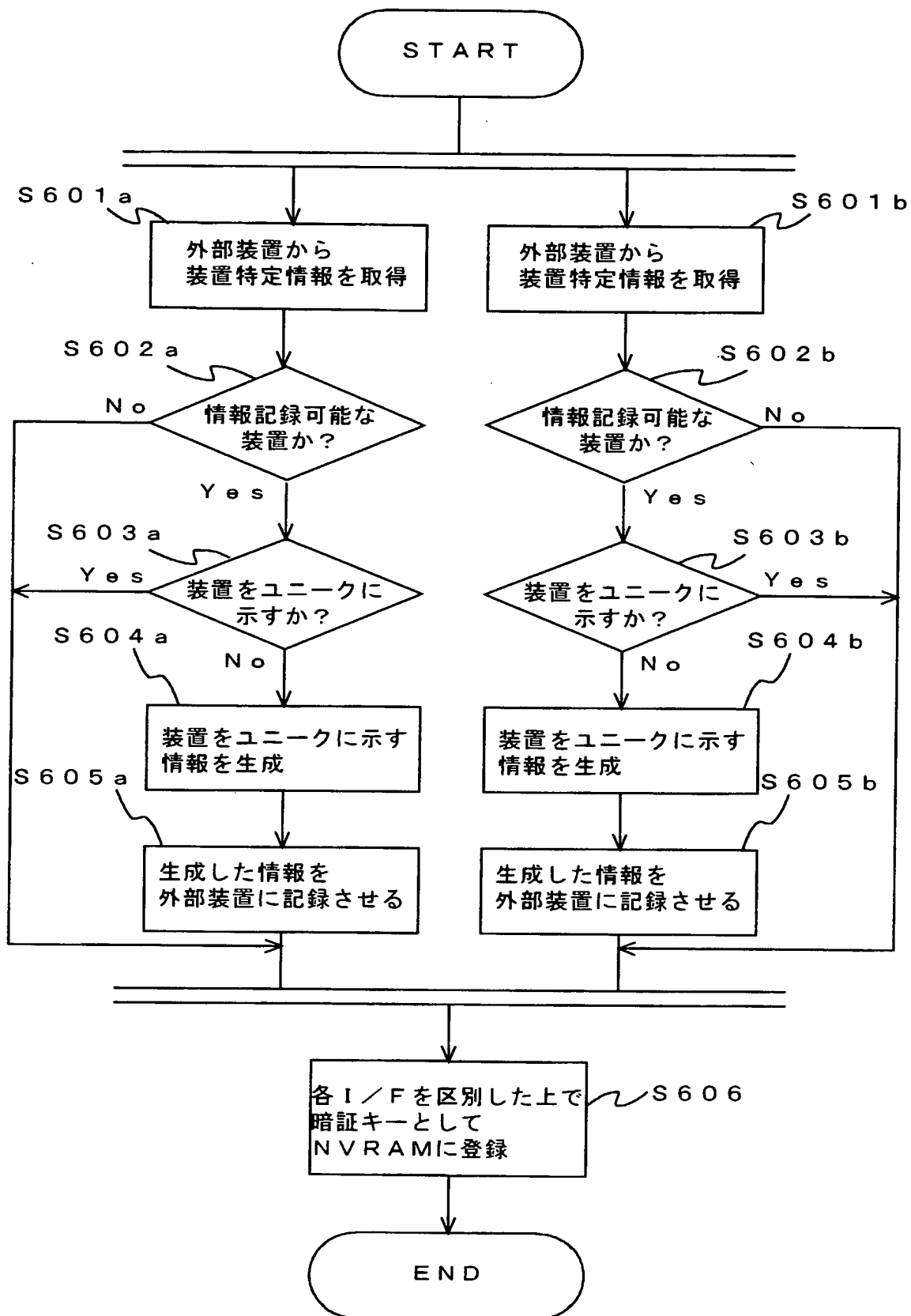


【図 11】





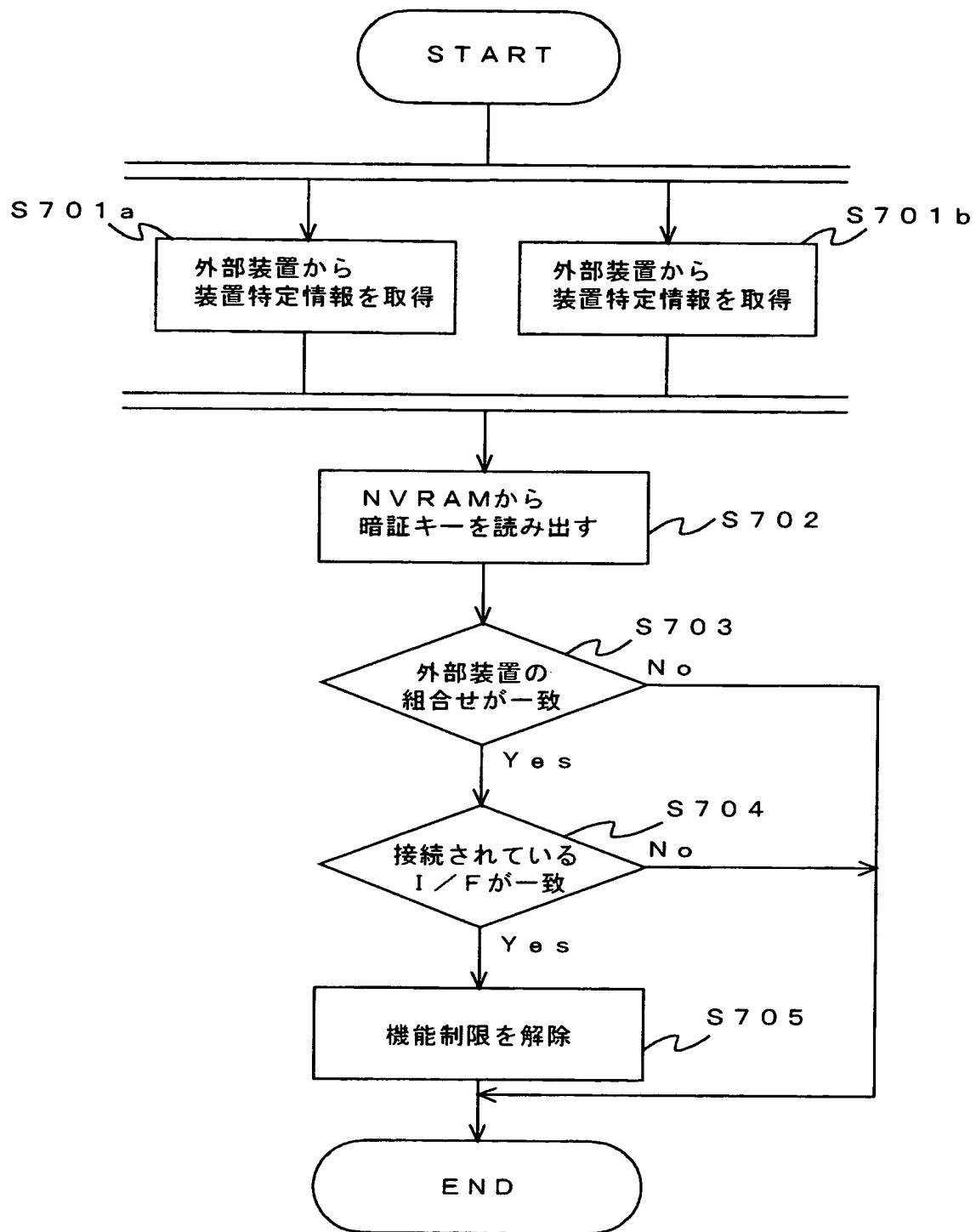
【図12】



【図 1 3】

暗証キー	
I / F	装置特定情報
A	C
B	D

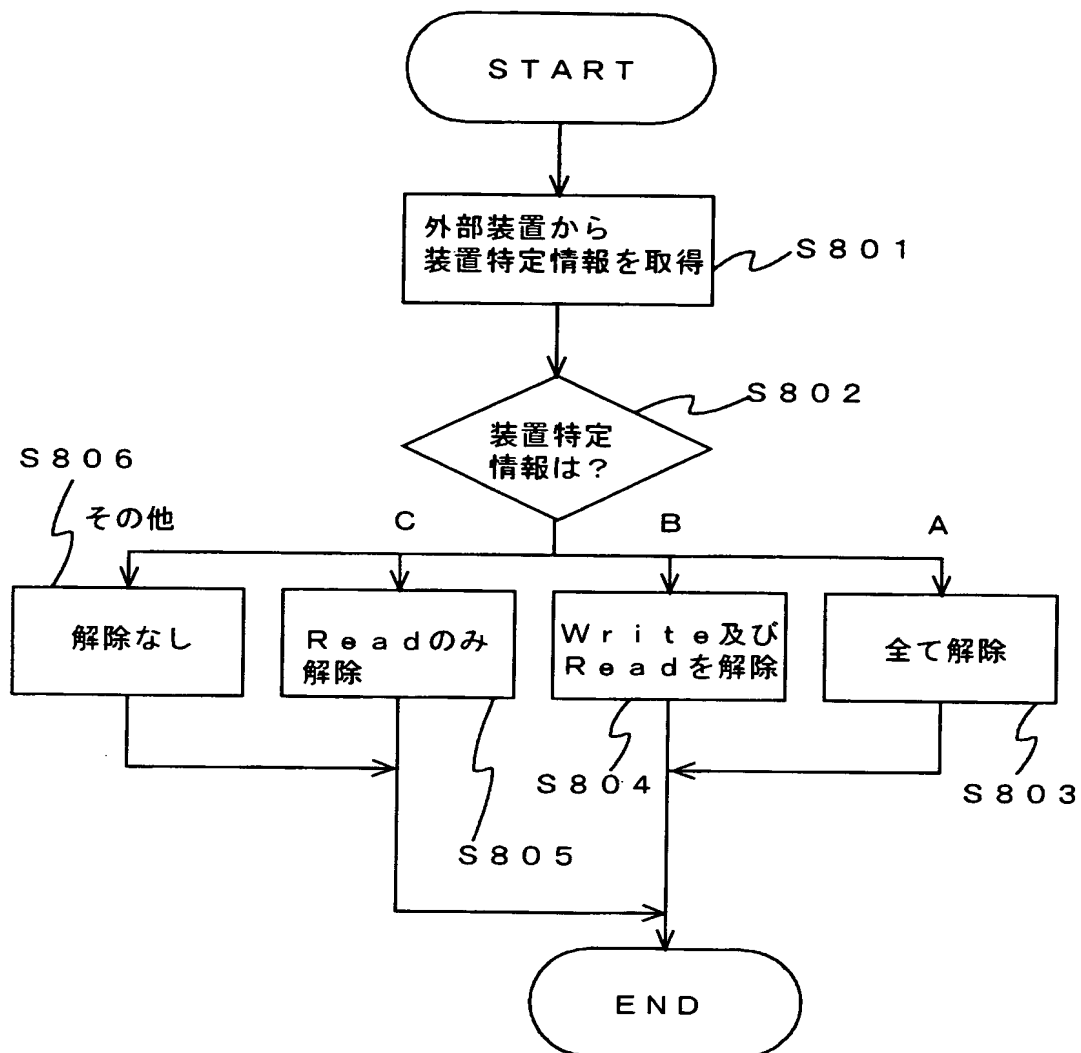
【図 14】



【図 15】

暗証キー	利用可能機能
A	A l l
B	R e a d , W r i t e
C	R e a d
D e f a u l t	N o t h i n g

【図 16】



【書類名】 要約書

【要約】

【課題】 不特定多数人が利用可能な環境に設置される電子機器の盗難を防止するとともに、電子機器に記憶された情報が盗用されることを防止する電子機器及びその不正利用防止方法並びにその不正使用防止プログラムを提供する。

【解決手段】 電子機器 100 が備える機能の少なくとも一部の実行を制限して使用不可とする機能制限を設定する動作制限部 102 と、外部装置を接続するための I/F 106 と、該 I/F 106 を介して接続された外部装置から該装置を特定する装置特定情報を取得する外部装置情報取得部 103 と、機能制限と所定の外部装置の装置特定情報とを関連づけて暗証キーとする書込制御部 107 と、該暗証キーを記憶する NVRAM 105 と、I/F 106 を介して接続されている外部装置から取得した装置特定情報が、NVRAM 105 に記憶されている暗証キーと一致するか否かを判断する比較部 104 とを有し、比較部 104 が一致すると判断した場合に、動作制限部 201 が機能制限を解除する。

【選択図】 図 3



特願 2002-231806

出 願 人 履 歴 情 報

識別番号

[300016765]

1. 変更年月日

2001年 4月 2日

[変更理由]

住所変更

住 所

東京都港区芝五丁目37番8号

氏 名

エヌイーシービューテクノロジー株式会社

2. 変更年月日

2003年 3月31日

[変更理由]

名称変更

住 所

東京都港区芝五丁目37番8号

氏 名

NECビューテクノロジー株式会社